International Journal of Intelligent Communication and Computer Science
Vol. 2, No. 2, 2024, Pages 17-26.

Enhancing Security with a Distributed Honeypot System Based on Blockchain: A Mathematical Attack Analysis

Neharika Nishad[1] and Rahul Singh[2]

[1]Research Scholar, Department of Computer Science and Engineering, Kanpur Institute of Technology, Affiliated to AKTU, Lucknow
[2]Department of Computer Science and Engineering, Kanpur Institute of Technology, Affiliated to AKTU, Lucknow

Research Paper

Email: nehariikanishad1@gmail.com
Received: 14 Mar 2024, Revised: 21 Aug 2024 Accepted: 20 Sep 2024

Abstract:

As cyber threats continue to evolve, the need for robust security measures becomes paramount. In this study, we propose a novel approach to enhance cybersecurity through the implementation of a distributed honeypot system built on blockchain technology. This system leverages the inherent security features of blockchain to create a resilient network of honeypots, capable of detecting and deterring malicious activities effectively. We conduct a comprehensive mathematical analysis of potential attacks targeting this distributed honeypot system, providing insights into its resilience and effectiveness against various cyber threats. Our findings underscore the potential of blockchain-based distributed honeypot systems as a proactive defense mechanism in the ever-evolving landscape of cybersecurity threats.

Keywords: Honeypot, Distributed system, Blockchain

1. Introduction

In the contemporary digital landscape, cybersecurity has emerged as a critical concern, with the proliferation of sophisticated cyber threats posing significant challenges to individuals, organizations, and nations alike [1]. As cyber attacks continue to evolve in complexity and scale, there is an urgent need for innovative and robust security solutions to safeguard against potential breaches and intrusions. Among the myriad of cybersecurity approaches, honeypot systems have gained prominence as an effective tool for detecting, monitoring, and mitigating malicious activities [2].

Traditionally, honeypots are decoy systems designed to lure cyber attackers into interacting with simulated vulnerabilities, thereby providing valuable insights into their tactics, techniques, and procedures (TTPs) [3]. However, the effectiveness of conventional honeypots is often limited by their centralized nature, making them susceptible to evasion and detection by sophisticated adversaries. To address these shortcomings, there is a growing interest in the development of distributed honeypot systems that leverage decentralized architectures, such as blockchain technology, to enhance resilience and scalability [4].

Blockchain, originally devised as the underlying technology powering cryptocurrencies like Bitcoin, has garnered widespread attention for its potential applications beyond financial transactions [5]. By employing cryptographic principles and distributed consensus mechanisms, blockchain enables the creation of tamper-proof and transparent ledgers, fostering trust and accountability in decentralized environments. Leveraging these attributes, researchers have begun exploring the integration of blockchain into cybersecurity frameworks, including distributed honeypot systems, to bolster their security and reliability.

Motivated by the need for innovative cybersecurity solutions, this paper proposes a distributed honeypot system based on blockchain technology. Our approach aims to harness the inherent security features of blockchain to create a resilient network of honeypots capable of detecting and mitigating cyber threats effectively. By distributing the honeypot infrastructure across multiple nodes within a blockchain network, we seek to enhance its robustness against evasion and detection by adversaries.

In this paper, we provide a comprehensive analysis of our proposed distributed honeypot system, focusing on its architecture, functionality, and security implications. Additionally, we conduct a mathematical analysis to evaluate its efficacy in detecting and deterring various cyber attacks, including reconnaissance, infiltration, and exfiltration attempts. Furthermore, we discuss the potential challenges and limitations of our approach and propose avenues for future research and development.

2. Honeypot and Blockchain

2.1 Honeypot System

In the realm of cybersecurity, honeypots have emerged as a valuable tool for detecting and analyzing malicious activities [6]. Honeypots are decoy systems designed to mimic legitimate assets or services within a network, enticing cyber attackers to interact with them. By monitoring and analyzing the activities directed at these decoy systems, security practitioners can gain valuable insights into the tactics, techniques, and procedures employed by adversaries. Traditional honeypots are typically deployed as standalone entities, often centralized within a network, which can make them susceptible to evasion and detection by sophisticated attackers. However, the evolution of cyber threats has spurred the development of more advanced honeypot architectures, including distributed honeypot systems.

Notable Papers

Li, Yang et. al [7] This paper presents a game-theoretic analysis of distributed honeypots, focusing on strategic interactions between attackers and defenders in a cybersecurity context. By modeling the interaction as a game, the authors investigate optimal strategies for both attackers attempting to evade detection and defenders seeking to detect and mitigate attacks. The study provides insights into the effectiveness of distributed honeypots in deterring malicious activities and highlights the importance of game theory in understanding and mitigating cyber threats.

Shi, Leyi et.al [8] This paper proposes a dynamic distributed honeypot system based on blockchain technology to enhance cybersecurity defenses. The authors leverage blockchain's decentralized and immutable ledger to distribute honeypot instances across a network, enabling real-time updates and adaptability to evolving threats. The study demonstrates the effectiveness of the blockchain-based approach in detecting and mitigating cyber-attacks, highlighting its potential for improving the resilience of honeypot systems.

H. Arun [9] This paper introduces Honeymesh, a novel approach for preventing distributed denial of service (DDoS) attacks using virtualized honeypots. The author presents a virtualized honeypot architecture capable of dynamically scaling and adapting to mitigate DDoS attacks effectively. Through extensive experimentation and evaluation, the study demonstrates the efficacy of Honeymesh in thwarting DDoS attacks and protecting network infrastructure from disruptions caused by malicious actors.

Wang et. al. [10] This paper proposes a strategic honeypot game model specifically tailored for mitigating distributed denial of service (DDoS) attacks in smart grid environments. The authors analyze the strategic interactions between attackers and defenders within the context of the smart grid infrastructure, considering the unique challenges and requirements of this domain. Through theoretical modeling and simulation studies, the study provides insights into effective defense strategies against DDoS attacks in smart grid deployments.

Miao and Wang [11] This paper presents an SDN-enabled pseudo-honeypot strategy for mitigating distributed denial of service (DDoS) attacks in the industrial Internet of Things (IIoT) environment. The authors leverage software-defined networking (SDN) principles to dynamically deploy pseudo-honeypots and divert malicious traffic away from critical IIoT infrastructure. Through experimental validation and analysis, the study demonstrates the effectiveness of the proposed strategy in enhancing the resilience of IIoT systems against DDoS attacks.

Huang et. al [12] This paper introduces a distributed cloud honeypot architecture designed to detect and mitigate cyber threats in cloud computing environments. The authors propose a scalable and resilient architecture leveraging distributed cloud resources to deploy and manage honeypot instances. Through experimental evaluation and performance analysis, the study demonstrates the effectiveness of the distributed cloud honeypot architecture in detecting and responding to various types of cyber attacks targeting cloud infrastructure.

2.2 Blockchain System

Blockchain technology, originally devised as the backbone of cryptocurrencies like Bitcoin, has expanded its reach beyond finance. At its core, blockchain serves as a decentralized and immutable ledger, recording transactions across a network of nodes transparently and securely. Leveraging cryptographic principles and consensus mechanisms, blockchain ensures data integrity and builds trust in distributed environments. Its security properties, including immutability, transparency, and decentralization, make it attractive for bolstering cybersecurity solutions such as honeypot systems. Incorporating blockchain into cybersecurity strategies enhances resilience against evolving threats. Blockchain's decentralized architecture reduces reliance on single points of failure and centralized control, mitigating risks in distributed ecosystems. The immutability of blockchain records ensures tamper-proof transaction histories, enabling accurate attribution of malicious activities within honeypot systems. Additionally, blockchain's transparency facilitates real-time monitoring and auditing, empowering organizations to detect and respond to security breaches swiftly. Furthermore, blockchain-enabled honeypots offer secure platforms for collaborative threat intelligence sharing. By securely recording and sharing attack data on the blockchain, organizations can enhance their collective defense posture against sophisticated adversaries. This collaborative approach fosters a stronger, more unified response to cyber threats, ultimately contributing to a safer digital landscape.

Notable Papers

Liu et.al [13] This paper introduces B4SDC, a blockchain-based system designed for secure data collection in Mobile Ad-Hoc Networks (MANETs). The authors propose a novel approach to leverage blockchain technology for securely collecting and storing security-related data in MANETs, addressing the challenges of data integrity, reliability, and privacy. Through experimental evaluation and performance analysis, the study demonstrates the effectiveness of B4SDC in enhancing the security and reliability of data collection in MANETs.

Sun et.al [14] This paper presents a blockchain-based IoT access control system designed to enhance security, lightweight, and cross-domain compatibility in IoT environments. The authors propose a novel access control mechanism leveraging blockchain technology to ensure secure and decentralized access management for IoT devices across diverse domains. Through experimental validation and analysis, the study demonstrates the feasibility and effectiveness of the proposed blockchain-based access control system in addressing security challenges in IoT deployments.

Leng et. al. [15] This paper provides a comprehensive survey of blockchain security techniques and research directions, focusing on addressing security challenges and vulnerabilities in blockchain systems. The authors present an overview of existing security mechanisms and explore emerging research directions for enhancing the security and resilience of blockchain networks. Through a systematic review of literature, the study offers insights into the current state-of-the-art in blockchain security and identifies future research directions in this rapidly evolving field.

Berdik et. al. [16] This paper presents a survey on the use of blockchain technology for information systems management and security. The authors review existing literature and discuss the applications of blockchain in various domains, including data management, authentication, and access control. Through a comprehensive analysis, the study highlights the potential benefits and challenges of integrating blockchain into information systems and offers insights into future research directions in this area.

Huaqun, and Yu [17] This paper provides a survey of blockchain technology and its security aspects, covering fundamental concepts, architectures, security mechanisms, and challenges. The authors review existing literature on blockchain security and discuss potential solutions to address security vulnerabilities and threats. Through a systematic analysis, the study offers a comprehensive overview of blockchain technology and its implications for security in various applications and domains.

Singh et. al. [18] This paper discusses blockchain security attacks, challenges, and solutions in the context of future distributed Internet of Things (IoT) networks. The authors examine potential security threats and vulnerabilities in blockchain-based IoT deployments and propose solutions to mitigate these risks. Through a comprehensive analysis, the study offers insights into the security implications of blockchain technology for distributed IoT networks and presents strategies to enhance their security posture.

In this paper, we explore the convergence of honeypot technology and blockchain to create a novel approach for bolstering cyber defenses. Our proposed distributed honeypot system leverages blockchain's decentralized architecture to distribute honeypot instances across a network of nodes, thereby enhancing their resilience against evasion and detection by adversaries. Through theoretical analysis and practical insights, we elucidate the potential benefits and challenges of integrating blockchain technology into honeypot-based cybersecurity frameworks.

3. Proposed Method

In Figure 1, the network portrayal illustrates the allocation of keys and states to individual nodes, distinguishing between Normal (N) and Honeypot (H) nodes. Each node possesses a unique key and is assigned a state based on its function within the network, either as a standard operational node or as a honeypot intended to entice and monitor malicious activities. This differentiation plays a pivotal role in the network's effective operation by enabling the identification and segregation of honeypot nodes from regular operational nodes.

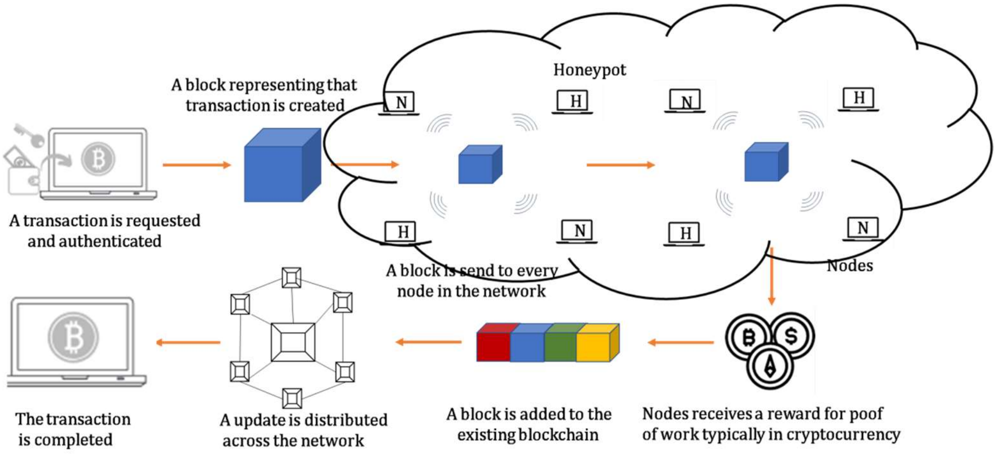
A block representing that transaction is created
Honeypot
N
H
N
H
A transaction is requested and authenticated
H
N
H
N
A block is send to every node in the network
Nodes
The transaction is completed
A update is distributed across the network
A block is added to the existing blockchain
Nodes receives a reward for poof of work typically in cryptocurrency

Figure 1: Schematic of Decentralized Honeypot system based on Blockchain Networks

During the initial operational phase, a symmetric key technique is employed to encrypt the records of each node within the network. This encryption process defines the cryptographic algorithm utilized to secure the node records. Symmetric key encryption entails the utilization of a single key for both data encryption and decryption, ensuring that only authorized parties possessing the key can access the encrypted information.

By leveraging symmetric key encryption in the initial phase, the network guarantees the confidentiality and integrity of node records, thereby safeguarding sensitive information against unauthorized access or tampering. This cryptographic technique introduces an additional layer of security to the network, effectively mitigating the risks associated with data breaches and unauthorized disclosures. Furthermore, the adoption of symmetric key encryption facilitates efficient and seamless communication between nodes, thereby enhancing the overall robustness and reliability of the network infrastructure.

In our system architecture, each node, whether classified as a Normal node or a Honeypot node, has the capability to participate in the same blockchain or different blockchains. It is a noteworthy observation that the resilience and security of a blockchain network tend to improve as the number of participating nodes increases. Consequently, in our proposed framework, we incorporate both Normal and Honeypot nodes within the same blockchain network to leverage this inherent property.

By integrating both types of nodes into a unified blockchain network, we aim to enhance the overall robustness and security posture of the system. The inclusion of Honeypot nodes within the blockchain not only contributes to the detection and monitoring of malicious activities but also strengthens the integrity and consensus mechanisms of the blockchain itself. Moreover, the coexistence of Normal and Honeypot nodes within the same blockchain fosters a collaborative environment where both types of nodes contribute to the network's collective resilience against cyber threats.

This approach offers several advantages, including increased transparency, fault tolerance, and immutability, which are fundamental properties of blockchain technology. Additionally, it enables seamless interoperability and communication between Normal and Honeypot nodes, facilitating the exchange of valuable information and insights to enhance cybersecurity defenses. Overall, the integration of both node types within the same blockchain network represents a strategic decision aimed at maximizing the effectiveness and efficiency of our system architecture in combating evolving cyber threats.

3.1 Mathematical Modeling for Attack Prediction

Let us assume a intruder start a attack then the likelihood of the intruder achieving success is represented by the probability of

$$s_c(a) = ps_c(a+1) + qs_c(a-1) \tag{1}$$

where a and c are bounded such that $0 \le a \le c$,

In the above given equation, p defines the winning probability, while $q = 1 - p$ is the loosing probability of a person. Due to the fact that equation (1) is a second order linear ordinary differential equation. Hence, initially a solution form $s_c(a) = z^a$ has to be assumed for some unknown base value z . Now, on substituting the form into (1), we have:

$$z^a = pz^{a+1} + qz^{a-1} \tag{2}$$

It must be noted here that the value of z should not be equal to 0.As a result, the equation (2) can factor out a common z^{a-1} . Now,

$$pz^2 - z + q = 0 \tag{3}$$

So $z = 1$ and $z = \frac{1}{p} - 1 = \frac{q}{p}$. Consequently, the solution of (1) is

$$s_c(a) = C_1(1)^a + C_2\left(\frac{q}{p}\right)^a \tag{4}$$

It begins when the attack transaction becomes part of the blockchain. During this phase, the honest chain extends by z blocks, denoted as $z \in \mathrm{N}$, while the attacker's chain extends by k blocks, where $k \in \mathrm{N}$. Notably, k can range from 0 to positive infinity. If k exceeds z , the attack succeeds; otherwise, if k is less than or equal to z , the attack fails. However, the scenario remains precarious even if the number of blocks the attacker is behind, denoted as *z*, is less than or equal to the number of blocks *k* mined by the honest network.

In such cases, the attacker still maintains the opportunity to catch up. The process of determining the probability of the attacker eventually catching up from z blocks behind closely resembles a classical problem in probability theory known as the Gambler's Ruin Problem. This parallel leads to the derivation of equation (5) as outlined in reference [19]. This equation encapsulates the likelihood of the attacker successfully overtaking the honest network despite starting from a disadvantaged position *z* blocks behind. By drawing parallels to the Gambler's Ruin Problem, researchers can better understand and model the dynamics of blockchain security in scenarios where attackers seek to overcome the honest network's lead and assert control over the network's consensus mechanism.

$$q_z = \begin{cases} 1 & if\ p \le q \\ \left(\dfrac{q}{p}\right)^2 & if\ p > q \end{cases} \tag{5}$$

In this given equation, *p* represents the probability of an honest node discovering the next block, while *q* indicates the probability of the attacker finding the next block. Furthermore, q_z denotes the probability of the attacker eventually catching up from bb blocks behind. These parameters play crucial roles in determining the dynamics of blockchain consensus mechanisms, particularly in scenarios where the attacker seeks to overcome a disadvantageous position and assert control over the network. Considering the range of possibilities for k from 0 to positive infinity—there are infinite scenarios where the attack succeeds. Hence, we opt to compute ($1 - P_{attack\ failure}$) instead.

The Poisson distribution serves as a fundamental probability distribution in statistics, particularly in scenarios involving the occurrence of rare events or events happening randomly over time or space. Formally, it expresses the probability of a specified number of events occurring within a fixed interval, under the assumption that these events happen independently and at a constant average rate known as the mean rate. The extension of the honest chain by z blocks represents a $fixed\ time\ interval$, while each instance of the attacker chain extending by one block constitutes an individual event. Consequently, the probability of each distinct value of k occurring is represented as:

$$P_{every\ different\ k\ appears} = \frac{\lambda^k e^{-\lambda}}{k!} \tag{6}$$

The variable k is the expected value. Let's suppose that the honest chain aims to extend by z blocks with a probability of *p*. In this scenario, the total duration required for the honest chain to extend by z blocks is governed by a Poisson distribution with a mean of z / p. Within this same time frame of z / p, the attacker chain can generate, on average $\lambda = z / p.q = \dfrac{zq}{p}$ blocks.

If z exceeds *k*, it indicates that the attacker's chain extends more blocks than the honest chain. Consequently, the attack on the chain is deemed successful, resulting in $(1 - P_{attack\ failure})$ being equal to 1.

However, when z is less than or equal to k, the probability that the attacker's chain can still bridge the gap from $z - k$ blocks behind is given by $\left(\dfrac{z}{p}\right)^{(z-k)}$, while the probability that the attacker's chain cannot catch up is

$$P_{can't\,catch\,up} = 1 - \left(\frac{q}{p}\right)^{(z-k)} \tag{7}$$

As per (5) and (6), we have

$$P_{every\ different\ k\ attack\ failure} = P_{every\ different\ k\ appears} . P_{can't\ catch up}$$

$$= \frac{\lambda^k e^{-\lambda}}{k!} . \left(1 - \left(\frac{q}{p}\right)^{(z-k)}\right) \tag{8}$$

Now,

$$P_{attack\ failure} = \sum_{k=0}^{z} P_{every\ different\ k\ attack\ failure} = \sum_{k=0}^{z} \frac{\lambda^k e^{-\lambda}}{k!} . \left(1 - \left(\frac{q}{p}\right)^{(z-k)}\right) \tag{9}$$

At last, we have

$$P_{attack\ successful} = 1 - P_{attack\ failure} = \sum_{k=0}^{z} \frac{\lambda^k e^{-\lambda}}{k!} . \left(1 - \left(\frac{q}{p}\right)^{(z-k)}\right) \tag{10}$$

4. Results

The results presented in the Figure 2 show the relationship between the number of nodes in a network and the corresponding attack probability with q= 0.1. As the number of nodes increases, the attack probability decreases exponentially. This trend suggests that larger networks with more nodes are significantly more resilient to attacks compared to smaller networks. For instance, when there are only 5 nodes in the network, the attack probability is relatively high at 9.13×10^{-4}. However, as the number of nodes increases to 10, the attack probability decreases drastically to 1.24×10^{-6}. This pattern continues as the number of nodes further increases, with the attack probability diminishing exponentially. By the time the network reaches 25 nodes, the attack probability is extremely low at 3.3×10^{-15}, indicating a highly secure and robust network configuration. These results highlight the importance of network scalability and size in mitigating the risk of attacks. Larger networks offer greater diversity and redundancy, making them inherently more resilient to malicious activities.

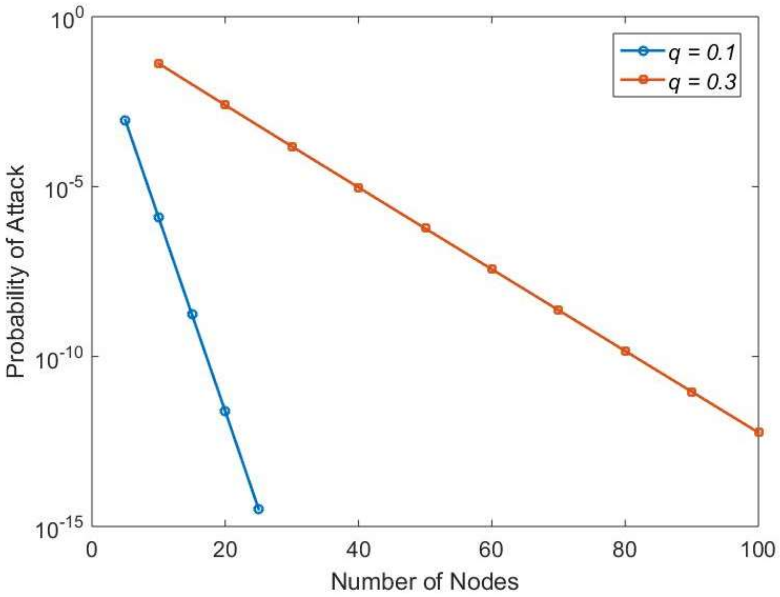

Figure 2: Probability of attack vs. number of nodes

The results presented in the Figure 2, demonstrate a clear correlation between the number of nodes in a network and the associated attack probability, assuming a fixed probability of attack at q = 0.3. As the number

of nodes increases, the likelihood of a successful attack decreases exponentially. This inverse relationship underscores the significance of network size and scalability in enhancing security against malicious activities.
For instance, with only 10 nodes in the network, the attack probability is relatively high at 0.042. However, as the network expands to 100 nodes, the attack probability diminishes significantly to 5.81×10^{-13}, indicating a highly secure network configuration. This substantial decrease in attack probability highlights the resilience of larger networks, which offer greater diversity and redundancy, thereby making it more challenging for attackers to exploit vulnerabilities.

Furthermore, the exponential decrease in attack probability as the number of nodes increases underscores the importance of network scalability in mitigating security risks. Larger networks not only provide more potential targets for attackers but also distribute the impact of attacks more widely, minimizing the likelihood of successful breaches.

Overall, these results emphasize the critical role of network size and scalability in bolstering cybersecurity defenses. By understanding and leveraging the relationship between network size and attack probability, organizations can design and deploy resilient networks capable of withstanding a wide range of cyber threats.

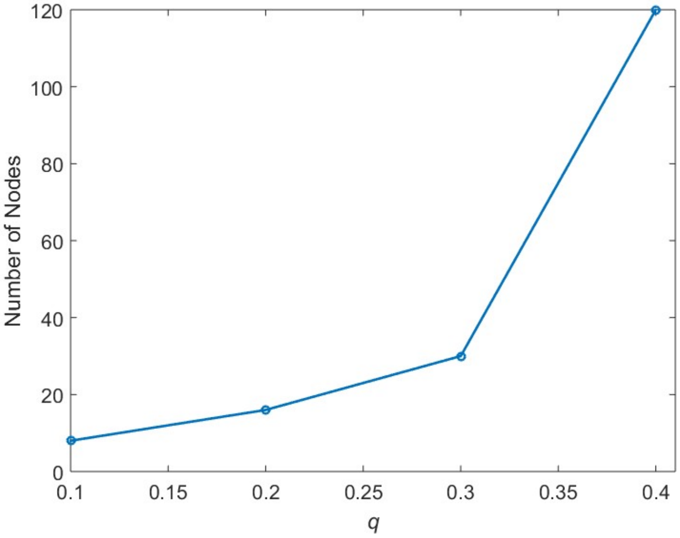

Figure 3: Number of Nodes vs. Probability of attack

The Figure 3 presents the relationship between the probability of attack and the corresponding number of nodes required to maintain the attack probability below a threshold of 0.0001. As the probability of attack increases, the number of nodes needed to achieve this threshold also rises, demonstrating the escalating security challenge posed by higher probabilities of attack.

For instance, with a relatively low probability of attack at 0.1, only 8 nodes are needed to ensure that the attack probability remains below 0.0001. However, as the probability of attack doubles to 0.2, the required number of nodes also doubles to 16. This trend continues, with higher probabilities of attack necessitating larger networks to maintain the desired level of security.

At a probability of attack of 0.3, the required number of nodes increases further to 30, indicating the significant impact of higher probabilities on network security requirements. This result underscores the importance of considering not only the likelihood but also the severity of potential attacks when designing and securing network infrastructures.

The exponential increase in the required number of nodes becomes more pronounced as the probability of attack reaches 0.4, where a substantial network size of 120 nodes is needed to maintain the attack probability below the specified threshold. This emphasizes the critical importance of proactive security measures and robust network defenses in mitigating the risks associated with higher probabilities of attack.

In summary, the results highlight the escalating security challenges posed by higher probabilities of attack, underscoring the need for organizations to implement comprehensive cybersecurity strategies and allocate resources accordingly to safeguard against potential threats.

5. Conclusion

In conclusion, our study emphasizes the critical importance of robust security measures in addressing the evolving landscape of cyber threats. Through the implementation of a distributed honeypot system built on blockchain technology, we propose a novel approach to enhancing cybersecurity. By leveraging the inherent security features of blockchain, our system creates a resilient network of honeypots capable of effectively detecting and deterring malicious activities.

Our comprehensive mathematical analysis of potential attacks targeting the distributed honeypot system provides valuable insights into its resilience and effectiveness against various cyber threats. The results demonstrate a clear correlation between the number of nodes in the network and the corresponding attack probability, highlighting the importance of network scalability in mitigating security risks. As evidenced by our findings, blockchain-based distributed honeypot systems offer significant potential as proactive defense mechanisms against cyber threats. By integrating blockchain technology into honeypot frameworks, organizations can enhance their cybersecurity posture and mitigate the risks associated with evolving threats.

References

1. Bécue, Adrien, Isabel Praça, and João Gama. "Artificial intelligence, cyber-threats and Industry 4.0: Challenges and opportunities." *Artificial Intelligence Review* 54, no. 5 (2021): 3849-3886.
2. Tsiknas, Konstantinos, Dimitrios Taketzis, Konstantinos Demertzis, and Charalabos Skianis. "Cyber threats to industrial IoT: a survey on attacks and countermeasures." *IoT* 2, no. 1 (2021): 163-186.
3. Javadpour, Amir, Forough Ja'fari, Tarik Taleb, Mohammad Shojafar, and Chafika Benzaïd. "A Comprehensive Survey on Cyber Deception Techniques to Improve Honeypot Performance." *Computers & Security* (2024): 103792.
4. Franco, Javier, Ahmet Aris, Berk Canberk, and A. Selcuk Uluagac. "A survey of honeypots and honeynets for internet of things, industrial internet of things, and cyber-physical systems." *IEEE Communications Surveys & Tutorials* 23, no. 4 (2021): 2351-2383.
5. Gorkhali, Anjee, Ling Li, and Asim Shrestha. "Blockchain: A literature review." *Journal of Management Analytics* 7, no. 3 (2020): 321-343.
6. Franco, Javier, Ahmet Aris, Berk Canberk, and A. Selcuk Uluagac. "A survey of honeypots and honeynets for internet of things, industrial internet of things, and cyber-physical systems." *IEEE Communications Surveys & Tutorials* 23, no. 4 (2021): 2351-2383.
7. Li, Yang, Leyi Shi, and Haijie Feng. "A game-theoretic analysis for distributed honeypots." *Future Internet* 11, no. 3 (2019): 65.
8. Shi, Leyi, Yang Li, Tianxu Liu, Jia Liu, Baoying Shan, and Honglong Chen. "Dynamic distributed honeypot based on blockchain." *IEEE Access* 7 (2019): 72234-72246.
9. Deshpande, Hrishikesh Arun. "Honeymesh: Preventing distributed denial of service attacks using virtualized honeypots." *arXiv preprint arXiv:1508.05002* (2015).
10. Wang, Kun, Miao Du, Sabita Maharjan, and Yanfei Sun. "Strategic honeypot game model for distributed denial of service attacks in the smart grid." *IEEE Transactions on Smart Grid* 8, no. 5 (2017): 2474-2482.
11. Du, Miao, and Kun Wang. "An SDN-enabled pseudo-honeypot strategy for distributed denial of service attacks in industrial Internet of Things." *IEEE Transactions on Industrial Informatics* 16, no. 1 (2019): 648-657.
12. Huang, Jason Xiaojun, Shikun Zhou, Nick Savage, and Weicong Zhang. "A distributed cloud Honeypot architecture." In *2021 IEEE 45th Annual Computers, Software, and Applications Conference (COMPSAC)*, pp. 1176-1181. IEEE, 2021.
13. Liu, Gao, Huidong Dong, Zheng Yan, Xiaokang Zhou, and Shohei Shimizu. "B4SDC: A blockchain system for security data collection in MANETs." *IEEE transactions on big data* 8, no. 3 (2020): 739-752.
14. Sun, Shuang, Rong Du, Shudong Chen, and Weiwei Li. "Blockchain-based IoT access control system: towards security, lightweight, and cross-domain." *IEEE Access* 9 (2021): 36868-36878.

15. Leng, Jiewu, Man Zhou, J. Leon Zhao, Yongfeng Huang, and Yiyang Bian. "Blockchain security: A survey of techniques and research directions." *IEEE Transactions on Services Computing* 15, no. 4 (2020): 2490-2510.
16. Berdik, David, Safa Otoum, Nikolas Schmidt, Dylan Porter, and Yaser Jararweh. "A survey on blockchain for information systems management and security." *Information Processing & Management* 58, no. 1 (2021): 102397.
17. Guo, Huaqun, and Xingjie Yu. "A survey on blockchain technology and its security." *Blockchain: research and applications* 3, no. 2 (2022): 100067.
18. Singh, Saurabh, ASM Sanwar Hosen, and Byungun Yoon. "Blockchain security attacks, challenges, and solutions for the future distributed iot network." *IEEE Access* 9 (2021): 13938-13959.
19. Moravec, Jiří. "Financial Aspects of Global Payment Systems." (2023).